# Special SCADA Overview (aka “SCADA-Bowl”)

Matthew E. Luallen, Encari

mluallen@encari.com

ENCARI

SANS

# Game Plan

- Understanding the Risk (Known Examples of Vulnerabilities & Countermeasures)
- Critical Infrastructure Protection (Example Regulations)
- Simple Principles to Reflect Upon
- Risk, Key Takeaways, Q&A

ENCARI

SANS

# What are the plays of the game? Vulnerabilities and Countermeasures

# Man-in-the-Middle Attacks* (1 of 7)

- Attacker reads, inserts and modifies information without either party aware
  - Physical Layer
  - Datalink Layer
  - Network Layer
  - Application Layer
  - System Layer
  - Social Layer

- What can happen?
  - Incorrect information is conveyed to the operator in a trusted manner
  - Incorrect control settings are sent to the system in a trusted manner
- Control is completely taken over by attacker

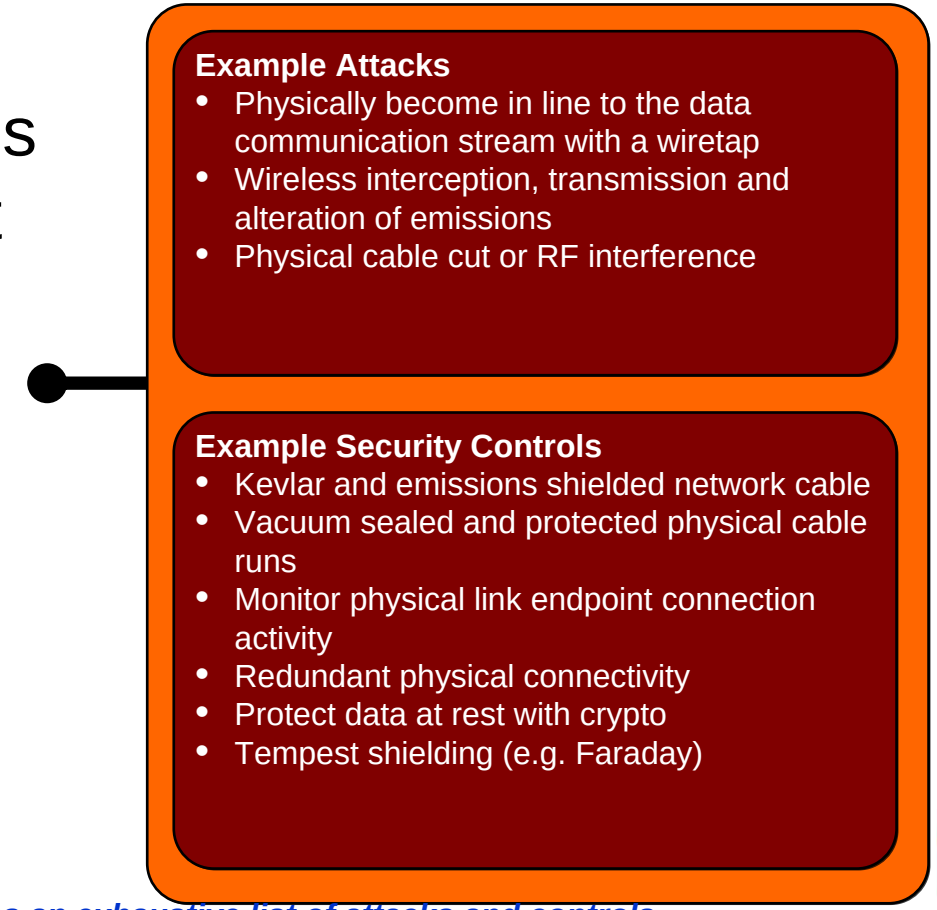
ENCARI

SANS

** Not to be considered as an exhaustive list of attacks and controls*

# Man-in-the-Middle Attacks* (2 of 7)

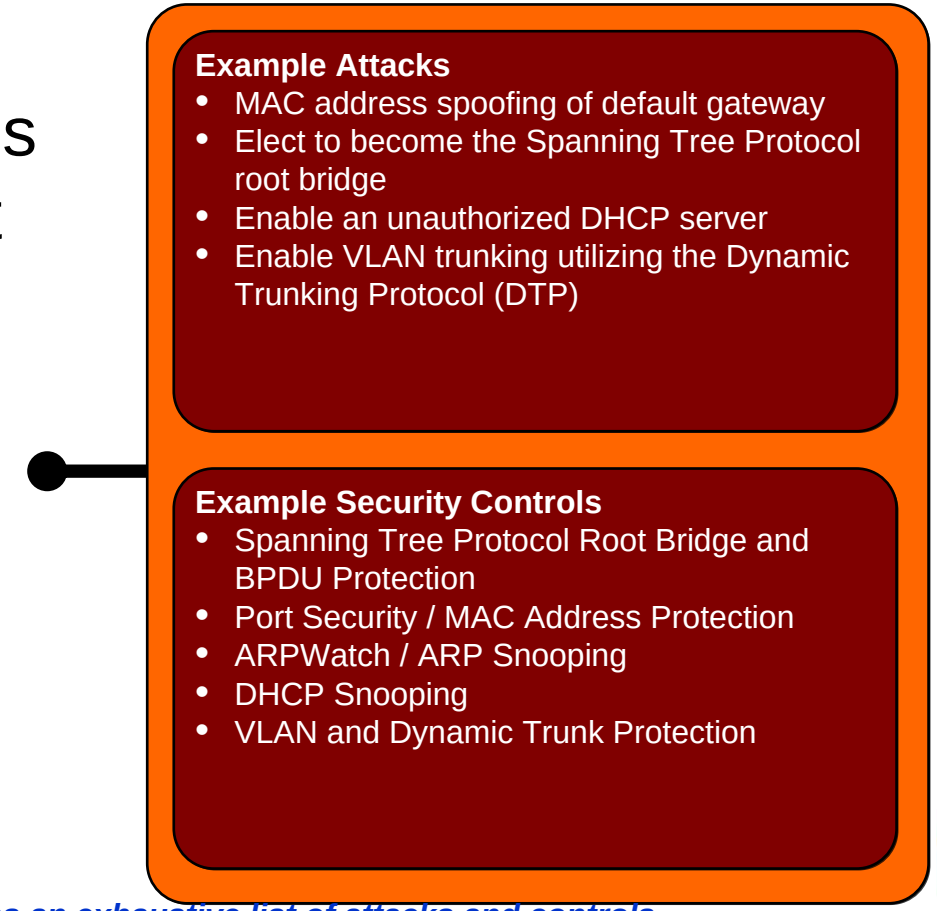
- Attacker reads, inserts and modifies information without either party aware
  - **Physical Layer**
  - Datalink Layer
  - Network Layer
  - Application Layer
  - System Layer
  - Social Layer




**** Not to be considered as an exhaustive list of attacks and controls***

# Man-in-the-Middle Attacks* (3 of 7)

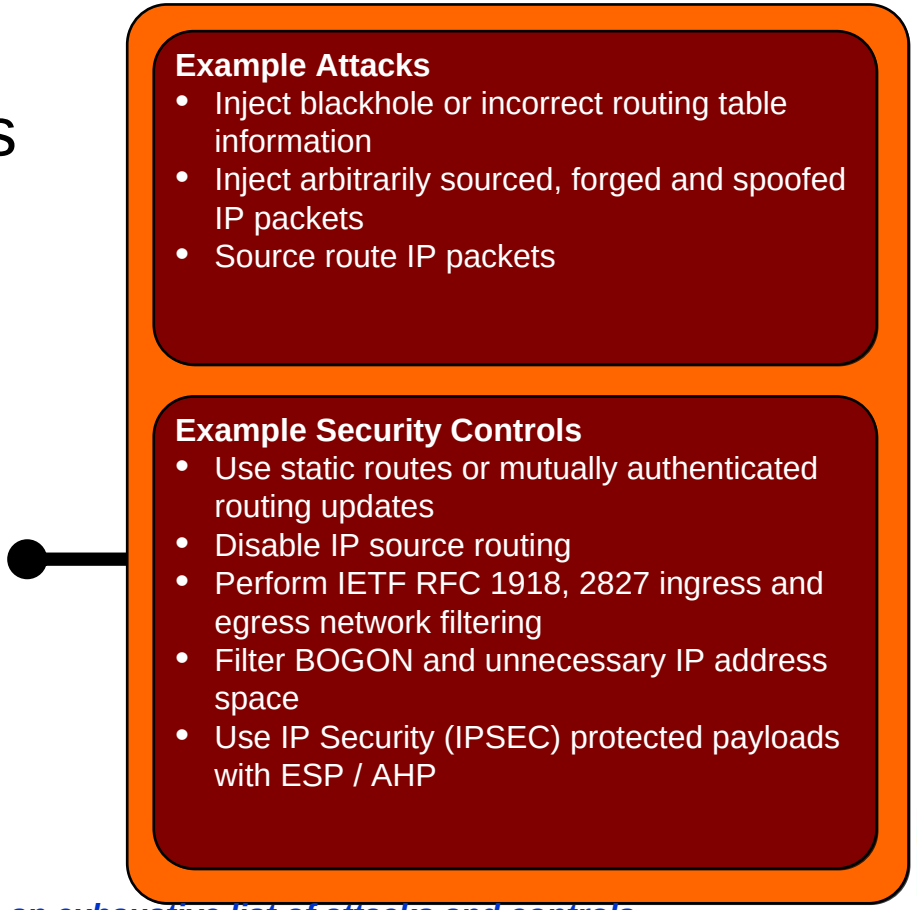
- Attacker reads, inserts and modifies information without either party aware
  - Physical Layer
  - **Datalink Layer**
  - Network Layer
  - Application Layer
  - System Layer
  - Social Layer




** Not to be considered as an exhaustive list of attacks and controls*

# Man-in-the-Middle Attacks* (4 of 7)

- Attacker reads, inserts and modifies information without either party aware
  - Physical Layer
  - Datalink Layer
  - **Network Layer**
  - Application Layer
  - System Layer
  - Social Layer




** Not to be considered as an exhaustive list of attacks and controls*

# Man-in-the-Middle Attacks* (5 of 7)

- Attacker reads, inserts and modifies information without either party aware
  - Physical Layer
  - Datalink Layer
  - Network Layer
  - **Application Layer**
  - System Layer
  - Social Layer

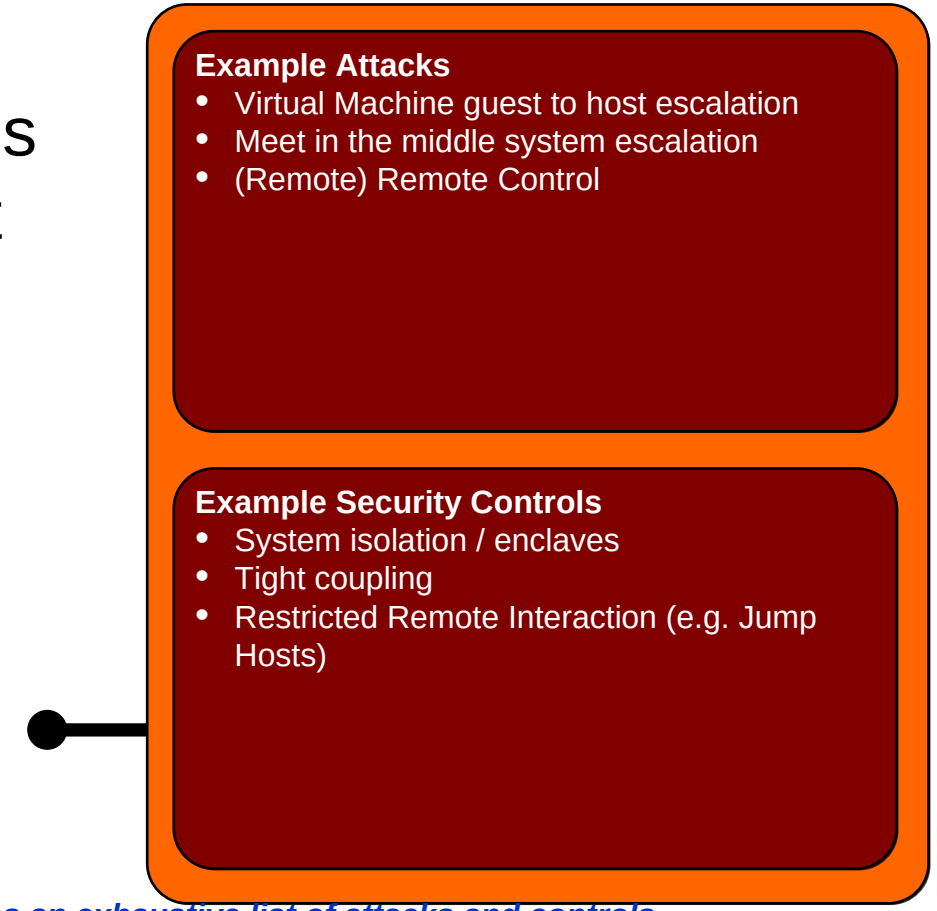
**Example Attacks**
- DNS cache poisoning
- Web browser cookie eavesdropping and manipulation
- Web browser cross site scripting / cross site request forgery
- Digital certificate impersonation
- Generic TCP Session Hijack

**Example Security Controls**
- Split DNS within enclaves
- Static host tables
- Trusted website browsing
- Contained application environments
- Stringent review of certificate trusts
- Limiting interdependencies
- Mutual Strong Authentication

**** Not to be considered as an exhaustive list of attacks and controls***

# Man-in-the-Middle Attacks* (6 of 7)

- Attacker reads, inserts and modifies information without either party aware
  - Physical Layer
  - Datalink Layer
  - Network Layer
  - Application Layer
  - **System Layer**
  - Social Layer




ENCARI

SANS

** Not to be considered as an exhaustive list of attacks and controls*

# Man-in-the-Middle Attacks* (7 of 7)

- Attacker reads, inserts and modifies information without either party aware
  - Physical Layer
  - Datalink Layer
  - Network Layer
  - Application Layer
  - System Layer
  - **Social Layer**

**Example Attacks**
- Phishing / Pharming / Whaling
- V-Phishing (Vishing)
- Telephone Calls
- Business Card / Name Dropping
- Identity Theft

**Example Security Controls**
- Party or Request Validation
- Identity Validation and Monitoring
- CAN SPAM Act
- Truth in Caller ID Act Legislation
- Legislation to alter processing of "Change of Address" forms

ENCARI

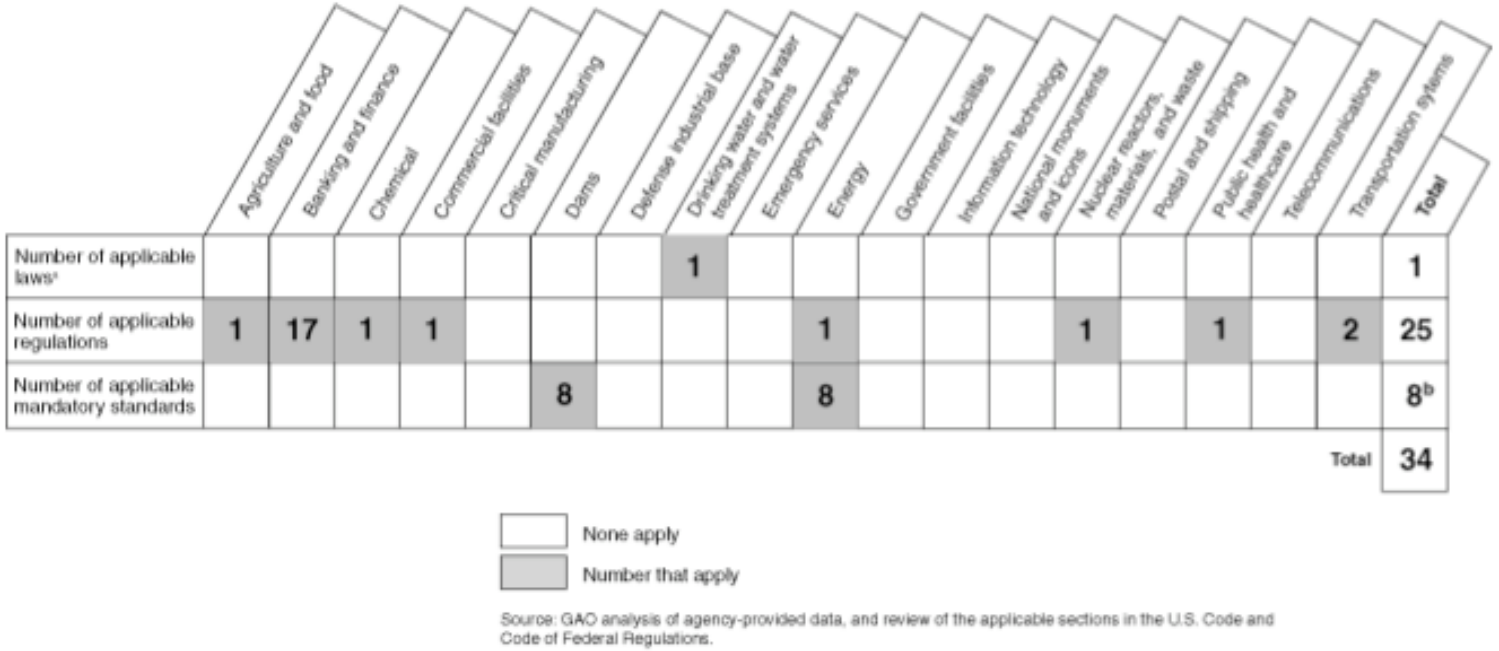
SANS

**** Not to be considered as an exhaustive list of attacks and controls***

# What are the rules of the game? Critical Infrastructure Protection

# Critical Infrastructure Federal Legal Requirements

**Figure 1: Summary of Federal Legal Requirements for Securing Privately Owned IT Systems and Data within Critical Infrastructure Sectors**



| | Agriculture and food | Banking and finance | Chemical | Commercial facilities | Critical manufacturing | Dams | Defense industrial base | Drinking water and water treatment systems | Emergency services | Energy | Government facilities | Information technology | National monuments and icons | Nuclear reactors, materials, and waste | Postal and shipping | Public health and healthcare | Telecommunications | Transportation systems | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Number of applicable laws[a] | | | | | | | | 1 | | | | | | | | | | | 1 |
| Number of applicable regulations | 1 | 17 | 1 | 1 | | | | | | 1 | | | | 1 | | 1 | | 2 | 25 |
| Number of applicable mandatory standards | | | | | | 8 | | | | 8 | | | | | | | | | 8[b] |
| | | | | | | | | | | | | | | | | | | Total | 34 |

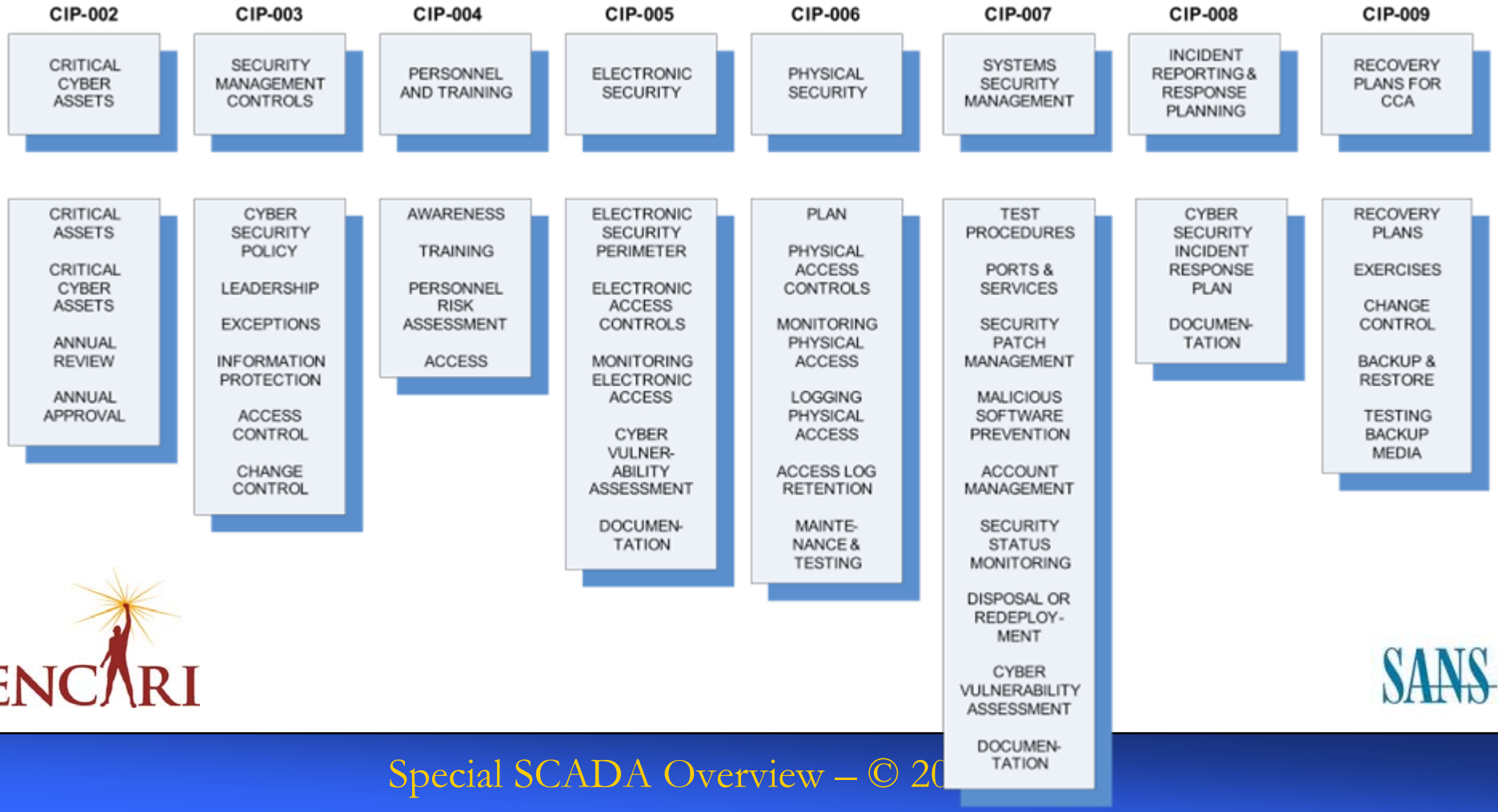
None apply

Number that apply

Source: GAO analysis of agency-provided data, and review of the applicable sections in the U.S. Code and Code of Federal Regulations.

**InformationTechnology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors, September 16, 2008 GAO Briefing**

# NERC CIP Reliability Standards (Regulated Requirements)




ENCARI

SANS

# CIP Past

- FERC SMD Appendix G
- NERC UAS-1200
- NERC 1300
- NERC CIP 002-009
- NERC CIP-001
- FERC Order 693
- FERC Staff Assessment
- FERC CIPS NOPR
- FERC Order 706

- Influential Factors
- NE Blackout 2003
- “Aurora”
- SANS CIA briefing
- News media in general

# CIPS In A Nutshell...

- ***Critical Infrastructure Protection*** *Standards (CIPS) are intended to protect the following:*
  - Bulk Power System (Bulk Electric System)
  - Critical Assets
    - Control Centers, Transmission Subs, Generation Plants
  - Critical Cyber Assets
    - EMS, DCS, RTUs, IEDs, PLCs, Relays
    - Decision Support Systems
  - Critical Infrastructure Information
- Provide greater reliability through greater security and accountability

ENCARI

SANS

# PENALTIES!
# The Cost of NERC CIP Non-Compliance

- Compromised reputation, potential loss of customers and business partners, ...
- Potentially a lot of money

**Appendix A: Base Penalty Amount Table**

The following lists the Base Penalty amounts corresponding to combinations of violation risk factor and violation severity factor.

| Violation Risk Factor | Violation Severity Level | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Lower | | Moderate | | High | | Severe | |
| | Range Limits | | Range Limits | | Range Limits | | Range Limits | |
| | Low | High | Low | High | Low | High | Low | High |
| Lower | $1,000 | $3,000 | $2,000 | $7,500 | $3,000 | $15,000 | $5,000 | $25,000 |
| Medium | $2,000 | $30,000 | $4,000 | $100,000 | $6,000 | $200,000 | $10,000 | $335,000 |
| High | $4,000 | $125,000 | $8,000 | $300,000 | $12,000 | $625,000 | $20,000 | $1,000,000 |

NOTE: This table describes the amount of penalty that could be applied for each day that a violation continues, subject to the considerations of Section 3.21 regarding frequency and duration of violations.

ENCARI

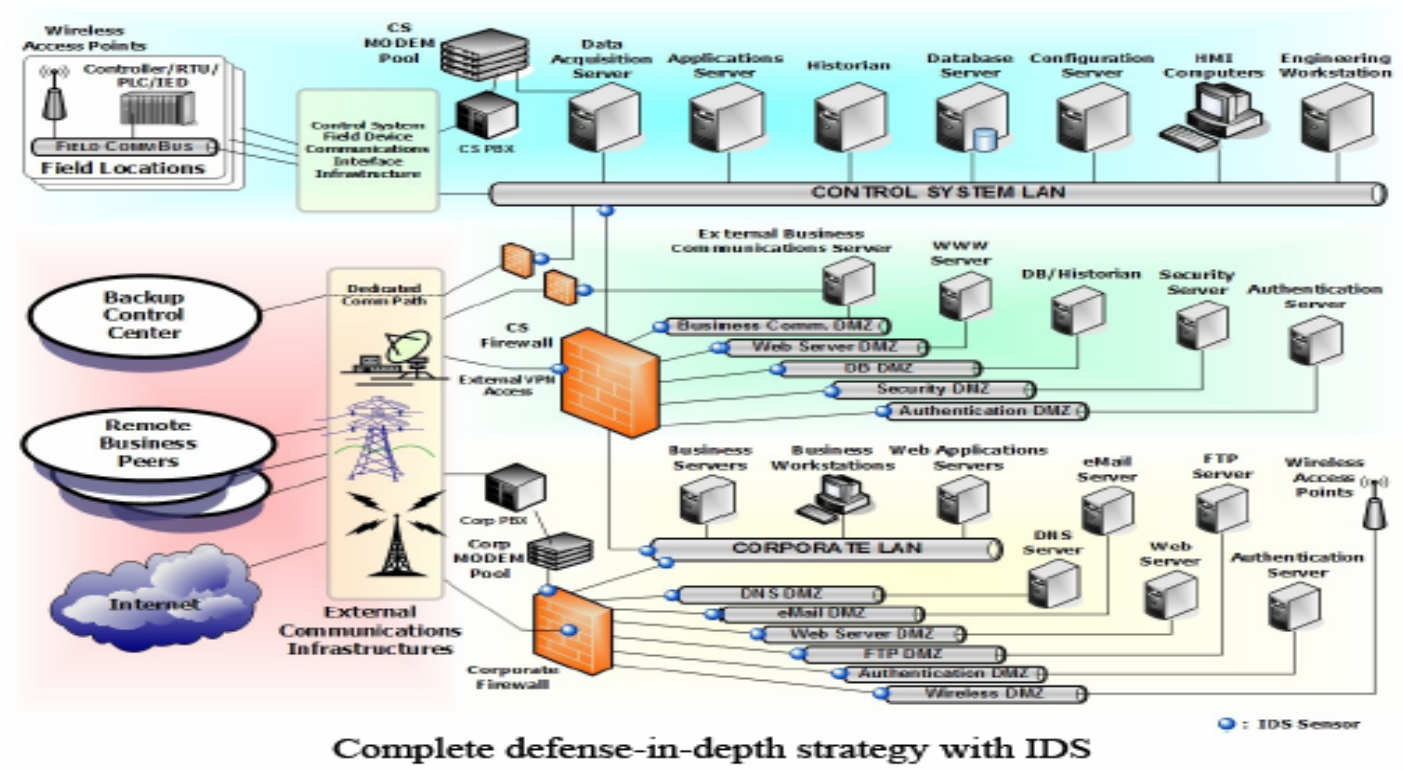
SANS

# International, National and Organizational Standards

- NERC CIP
- ISA S99
- ISO 27001
- NIST SP 800-53 r2, 800-82
- NRC
- IEC 62351
- NNSA
- DoD 8500.1
- IEEE P1686
- IEEE P1711
- IEC 61850 (Cigre B5.38)

http://www.us-cert.gov/control_systems/csstandards.html

# NIST SP 800-82 Example Architecture




Complete defense-in-depth strategy with IDS

Source: Idaho National Laboratory, Control Systems Cyber Security: Defense in Depth Strategies (May, 2006)

# Apply Vertical Intelligence of Other Critical Infrastructures

- Healthcare
  - Life supporting solutions
- Finance
  - Integrity of transaction
- Telecommunications
  - Robust, fault-tolerant communications system
- Electric Utilities (SCADA/DCS)
  - Safety, Reliability, System Criticality, Vendor Systems

# Simple Principles to reflect upon while architecting

# Simple Principles

- Isolationism provides protection
  - The more isolated an environment is from others the greater the success of physical and logical security controls assuring continuously accurate information and control

# Simple Principles

- Assets will be physically stolen or lost

  - Physical assets, physical assets storing electronic information and electronic assets will be stolen or lost
  - You must limit the impact of any theft of information

- Your conversations will be eavesdropped upon
  - Any verbal, paper or electronic conversation can be monitored; you must be accepting of this and utilize the appropriate protective controls to limit your risk




ENCARI

SANS

# Simple Principles

- Assets will be physically stolen or lost

- Physical assets, physical assets storing electronic information and electronic assets will be stolen or lost
- You must limit the impact of any theft of information

- Your conversations will be eavesdropped upon
  - Any verbal, paper or electronic conversation can be monitored; you must be accepting of this and utilize the appropriate protective controls to limit your risk


ENCARI

SANS

# Simple Principles

- Build with a moat (control)
  - Separate trust levels / Security Enclaves
  - Understand how the moat (control) works

* Nijo Castle
Kyoto, Japan

- (or) Build with Nightingale Floors *

ENCARI

SANS

# Air Gaps Not Only Answer

- “Computer Virus Strikes Space Station”
- August 27, 2008: Tariq Malik space.com
- A virus designed to swipe passwords from online gamers has inexplicably popped up in some laptop computers aboard the international space station.
- The low-risk virus was detected on July 25, but did not infect the space station's command and control computers and poses no threat to the orbiting laboratory, NASA officials said.

ENCARI

SANS

# Holistic Approach

- Threats, Vulnerabilities, and Consequences
- Standards and Regulations
- People, Process, and Technology


ENCARI

SANS

# Do you have a choice to play?
# Risk, Key Takeways and Q&A

# Encountered Themes of Risks

- Too much public information about the system
- Poor communication procedures throughout the industry regarding cyber security
- Growing interdependent, interconnected legacy systems
- Insufficient security awareness and security training
- Constrained ability to tactically execute and enforce documented policies, standards and procedures
- Attrition of workforce

ENCARI

SANS

# Key Takeaways

- Assure holistic and integrated involvement with people, processes and technology
- Maintain ongoing situational awareness operationally, physically and cyber (internally and externally)
- The discovery process may prove to be difficult – remember to understand all components including environmentals
- Key architecture components are crucial (electronic and physical perimeters, authentication, logging, remote management, change management, development, data storage, communication flow)
- Architect and build for incident response
- Defense in depth
- Security awareness and training to combat workforce attrition
- NERC CIP Reliability Standards are paving the way for future legislation and compliance requirements for international electric utilities and critical infrastructures

ENCARI

SANS

# Q&A

- Contact Information
  - Matthew Luallen – Co-Founder, Encari
    - 312-375-4715
    - mluallen@encari.com

- Visit our blog at Control Engineering magazine's website
  - www.controleng.com


ENCARI

SANS